Grenze International Journal of Engineering and Technology, January Issue

Block Chain based Certificate Transparency and Revocation Transparency

Manoj G[1] and K IndraSena Reddy[2]
[1-2]Dept. of MCA, RNS Institute of Technology Bengaluru. India
Email: manojg23mca@rnsit.ac.in, kethamreddyindrasenareddy23mca@rnsit.ac.in

***Abstract*— Digital certificate environment plays a critical role in secure communication over the internet. Nevertheless, it is susceptible to a lack of Certificate Transparency and Revocation Transparency solve these problems. This paper discusses how block chain technology can help improve CT and RT by providing a decentralized, immutable, and transparent record book for certificate life cycle management. We introduce existing solutions, their drawbacks, and suggest a block chain-based approach that enhances trust, accountability, and auditability in certificate issuance and revocation. In today's digital environment, secure communication and authentication rely mainly on the Public Key Infrastructure, specifically digital certificates issued by Certificate Authorities. Nonetheless, the classic PKI model suffers from its own shortcomings, such as certificate, weak revocation mechanisms, and Certificate Transparency and Revocation Transparency lack were therefore suggested to overcome these weaknesses through the availability of public logs of certificates issued and revoked. Nevertheless, these mechanisms tend to rely on centralized infrastructures, and this brings trust, availability, and integrity risks.**

I. INTRODUCTION

Digital certificates, mostly X.509 certificates, form the basis of HTTPS and other secure communication protocols. These certificates but this centralized model has long given rise to issues like fraudulent issuance and hidden certificate misuse. Certificate Transparency is a system launched to make available publicly all certificates so that domain owners and auditors can detect unauthorized certificates. CT does not effectively manage revocation information, though.

Block chain provides a plausible solution due to decentralization, as well as transparency. With block chain, we can record certificate issuance and revocation events in a distributed ledger, which can be publicly verified and tamper-proof. This paper explores the possibility and advantages of such a system.

Secure online communication is crucial in this internet-based age for safeguarding information, guaranteeing privacy, and upholding user and system trust. Central to all this security is the Public Key Infrastructure, which employs digital certificates to validate websites, encrypt traffic, and authenticate identities. These certificates are provided and controlled.

Though, in the last ten years, there have been several instances that exposed serious weaknesses of the classical PKI model. Many had been compromised in issuing bogus certificates. Once issued, users and systems do not have an instantaneous method to recognize or reject them unless they are subjected to active monitoring. Moreover, revocation systems like Certificate Revocation Lists and the Online Certificate Status Protocol have turned out to be ineffective, slow, and unreliable under some networking or performance scenarios.

Grenze ID: 01.GIJET.12.1.513_2

II. CHALLENGES

A. Scalability and Storage Overhead

Maintaining all certificate records issued and revoked on a block chain can result in substantial growth of data, particularly with large volumes of certificates issued daily.
Public block chains do not have high throughput and are expensive per transaction, which makes them unsuitable for high-frequency logging of certificates.

B. Latency and Real-Time Verification

Block chain networks introduce latency due to block confirmation times. The delay can interfere with real-time detection of revoked or fraudulent certificates.
Transparency of revocation calls for timely notification, which could be incompatible with block chain's typical average transaction time.

C. Block chain Transaction Cost

Public block chain writing normally entails gas fees or transaction fees. Recording every issuance of and revocation of a certificate can become costly, particularly for extensive domains with regular updates to certificates.

D. Privacy and Confidentiality

Logging certificate metadata to a public block chain can make sensitive data, like domain names, IP addresses, or internal systems, publicly visible.
Maintaining privacy without losing transparency is a hard act, particularly in heavily compliance-dominated industries like healthcare or finance.

III. LITERATURE SURVEY

Google's Certificate Transparency: Added append-only CT logs to identify certificates but did not include revocation tracking.
Revocation Transparency: Suggested a Merkle-tree based revocation log in combination with CT, but was centralized.
Cert Ledger: A block chain-based PKI system for controlling certificates and revocations with smart contracts.
AKI: Autonomous Key Infrastructure: Leverages block chain for automated management of the certificate life cycle, including revocation.

A. DTKI – Decentralized Trustworthy Key Infrastructure

Reference: E. et al. "Decentralizing PKI with block chain."
Contribution: Proposed a decentralized PKI model based on several log servers and monitors with responsibility through block chain.
Key Point: Offers and transparency without a single point of failure using block chain.

B. Trust Chain

Reference: Singh, A. et al. "Trust Chain: A Block chain Based Trust Management Framework Devices."
Contribution: Proposed a light weight block chain-based system for resource-limited devices.
Advantage: Introduces block chain for improved energy efficiency and scalability.

C. Block PKI

Reference: Tomescu, A. & Devadas, S. (2018). "Catena: Efficient Non-equivocation via Bitcoin."
Contribution: Employs Bitcoin block chain to maintain crypt graphic proofs of certificate issuance.
Innovation: Prevents CAs from equivocating (issuing varying certificates to varying parties).

D. EthIKS-Ethereum-based Infrastructure for Key Management

Contribution: Employs smart contracts to govern certificate life cycles, such as validation and revocation.
Highlight: Showcases a full life-cycle end-to-end certificate management system with public block chain technology.

E. Sovrin and Hyper ledger Indy Projects

Context: Define self-sovereign identity, encompassing block chain-based certificate issuance and openness.

Relevance: Although not primarily centered around CT, these projects introduce sophisticated ideas such as selective disclosure and revocable credentials through block chain.

IV. Stake Holders

A. Certificate Authorities

Role: Issue digital certificates (X.509) to domain owners.
Involvement:
Send certificate issuance and revocation transactions to the block chain.
Ensure adherence to CT and RT protocols.
Interest: Preserve trust and compliance with minimal liability.

B. Domain Owners

Role: Request, administer, and track their domain certificates.
Involvement:
Ensure that only certified certificates have been issued for their domain.
Track block chain logs for unauthorized or revoked certificates.
Interest: Avoid abuse or unauthorized issuing of certificates for their domain.

C. End Users

Role: Dependent on digital certificates to make secure connections.
Involvement:
Only trust logged and valid certificates on the block chain.
Interest: Have secure, private, and authentic interaction with websites.

D. Block chain Network Participants

Role: Sustain the block chain infrastructure by confirming and documenting transactions.
Involvement:
Validate certificate issuance/revocation entries.
Secure the network via consensus mechanisms.
Interest: Gain rewards (if public block chain) and ensure network stability.

E. Auditors and Monitors

Role: Watch block chain logs constantly for anomalous behaviour or miss behaviour
Involvement:
Identify revoked certificates.
Notify domain owners or invalidate trust in compromised.
Interest: Increase trust, transparency, and security in the certificate ecosystem.

V. Conclusion

The existing Public Key Infrastructure is the key to providing secure internet communication, but it is not without inherent weaknesses specifically regarding the centralized trust model, susceptibility to certificate and incoherent revocation mechanisms. The development of Certificate Transparency was a forward step towards enhancing accountability in certificate issuance but lacks a strong and transparent revocation tracking mechanism. Such constraints have put users at risk of attacks like man-in-the-middle, unauthorized entry, and online impersonation.

Here, block chain technology provides a solution to plug the loopholes of both CT and Revocation Transparency. With the decentralization, immutability and transparency of block chain, a more secure, reliable, and effective certificate management system can be created. Block chain enables a publicly verifiable history of all certificate life cycle events such as issuance, renewal, expiration, and revocation. Moreover, smart contracts make it possible to automate important procedures and rid the world of trust in a central authority.

But this method also creates new problems. Scalability, transaction fees, privacy issues, and integration with existing PKI infrastructure are serious problems that need to be overcome before large-scale implementation is possible. block chain models, zero-knowledge proofs, off-chain storage, and hybrid models could possibly offset some of these disadvantages and make implementation more feasible and effective.

In the future, the integration of block chain and certificate transparency is a paradigm change for digital trust to be established and sustained. There should still be an ongoing exploration of privacy-preserving methods, cross-chain compatibility, and lightweight verification protocols to make this vision increasingly deployable in the real world.

REFERENCES

[1] Nudging Lifestyles for Better Health Outcomes.
[2] Reexamining the Nature of Learner Control.
[3] Combining Human and Machine Intelligence in Large Scale.
[4] Big data and Disease Prevention.
[5] www.jmir.org
[6] www.crowdsourcing.org
[7] The Statistics Portal. Number of smartphone users in the united states from 2010 to 2022. https://www.statista.com/statistics/201182/forecast-of-smartphone-users-in-the-us/.
[8] Fabio Assolini. Smishing and the rise of mobile banking attacks. https://securelist.com/smishing-and-the-rise-of-mobile-banking-attacks/75575/.
[9] Wenhao Liu, Shengbao Wang, Xiao Tan, Qi Xie, and Qizhen Wang. Identity-based one round key agreement protocol without bilinear pairings. In P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2015 10th International Conference on, pages 470–473. IEEE, 2015.
[10] Mohammad Sabzinejad Farash and Mahmoud Ahmadian Attari. A provably secure and efficient authentication scheme for access control in mobile pay-tv systems. Multimedia Tools and Applications, 75(1):405–424, 2016.
[11] Jia-Lun Tsai and Nai-Wei Lo. A privacy-aware authentication scheme for distributed mobile cloud computing services. IEEE systems journal, 9(3):805–815, 2015.
[12] Debiao He, Sherali Zeadally, Neeraj Kumar, and Jong-Hyouk Lee. Anonymous authentication for wireless body area networks with provable security. IEEE Systems Journal, 2016.